IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA, Plaintiff, v. ANTON PERAIRE-BUENO, and JAMES PERAIRE-BUENO, Defendants.	Case No.: 1:24-cr-00293-JGLC

DEFENDANTS' MEMORANDUM OF LAW IN SUPPORT OF JOINT MOTION TO SUPPRESS OR, ALTERNATIVELY, FOR *FRANKS* HEARING

TABLE OF CONTENTS

INTRODUCTION 1

BACKGROUND 1

ARGUMENT 2

I. LEGAL FRAMEWORK 2

II. DIAS INCLUDED MANY DELIBERATE FALSEHOODS IN HIS SWORN AFFIDAVITS OR, AT A MINIMUM, ACTED WITH RECKLESS DISREGARD FOR THE TRUTH. 4

A. Dias falsely asserted the Peraire-Buenos baited their alleged victims by proposing transactions that they had "no intention of executing." 5

B. Dias falsely accused the Peraire-Buenos of targeting "more obscure cryptocurrency tokens," even though the tokens at issue include some of the most valuable and common in the world. 8

C. Dias falsely characterized the alleged victims as traders who specialized in "cryptocurrency arbitrage," but in fact, they were "sandwich attackers" who engaged in harmful market manipulation. 9

D. Dias falsely claimed the Peraire-Buenos "altered transactions," but they are only accused of changing the *order* of requested transactions, not the terms.....11

E. Dias manipulated a publicly available diagram of the MEV Boost application on the Ethereum Network to omit critical information that undermines the fraud allegations. 12

F. Dias falsely claimed the Peraire-Buenos "tampered" with the blockchain itself, but as Dias must know, that is not technologically possible, and all the transactions at issue remain on the permanent, public ledger. 14

III. WITHOUT THE MANY FALSEHOODS THAT DIAS INCLUDED IN HIS AFFIDAVITS, PROBABLE CAUSE WAS LACKING TO ISSUE THE WARRANTS TO GOOGLE. 16

CONCLUSION 18

TABLE OF AUTHORITIES

Page(s)

CASES

Franks v. Delaware, 438 U.S. 154 (1978) ..... *passim*

United States v. Awadallah, 349 F.3d 42 (2d Cir. 2003) 16

United States v. Castellanos, 820 F. Supp. 80 (S.D.N.Y. 1993) 1

United States v. Fuccillo, 808 F.2d 173 (1st Cir. 1987) 3

United States v. Gratkowski, 964 F.3d 307 (5th Cir. 2020) 15

United States v. Lauria, 70 F.4th 106 (2d Cir. 2023) 3, 16

United States v. Leon, 468 U.S. 897 (1984) 3

United States v. Perez, 247 F. Supp. 2d 459 (S.D.N.Y. 2003) 3

Williams v. Binance, 96 F.4th 129 (2d Cir. 2024) 14, 15

OTHER AUTHORITIES

Dep't of Justice Press Release, Two Brothers Arrested for Attacking the Ethereum Blockchain and Stealing $25M in Cryptocurrency (May 15, 2024), https://www.justice.gov/opa/pr/two-brothers-arrested-attacking-ethereum-blockchain-and-stealing-25m-cryptocurrency 16

https://coinmarketcap.com/currencies/aave/ (last accessed Dec. 4, 2024) 9

https://coinmarketcap.com/currencies/shiba-inu/ (last accessed Dec. 4, 2024) 9

https://hackmd.io/@flashbots/HJ3EbzVUY (last accessed Dec. 4, 2024) 12

https://etherscan.io/tx/0x67f71374ec751676a807e8e874a6fe0482a9155220f97c61b00c2d1dba04ba00 (last accessed Dec. 6, 2024) 7

https://etherscan.io/tx/0x8ec2730e32319529ba084390e87c2f4384d69ce057bc1001daa6b8ac38be4ba9 (last accessed Dec. 6, 2024) 10

https://etherscan.io/tx/0xef7f6864a93f8d10dd8fafbe75b041db8c282159fe43632c26a29f176894678e (last accessed Dec. 6, 2024) 6

What is a Sandwich Attack, Uniswap, https://support.uniswap.org/hc/en-us/articles/19387081481741-What-is-a-sandwich-attack (last accessed Dec. 6. 2024) 12

W. LaFave, *Search and Seizure* § 4.4(c) (6th ed. 2021) 16

What is Etherscan and how to use it?, Coinbase, https://www.coinbase.com/learn/crypto-glossary/what-is-etherscan-and-how-to-use-it (last accessed Dec. 5, 2024) 6

INTRODUCTION

Intentionally or recklessly misleading a judge into issuing a search warrant is the sort "egregious misconduct" that "must be deterred" if the Fourth Amendment and its warrant requirement are to have "any meaning." *United States v. Castellanos*, 820 F. Supp. 80, 82 (S.D.N.Y. 1993) (Sotomayor, J.). Here, in applying for two search warrants to Google, LLC, Special Agent Marco Dias, of the Internal Revenue Service-Criminal Investigation, submitted sworn affidavits in which he deliberately made false statements or recklessly disregarded the truth about Defendants Anton Peraire-Bueno and James Peraire-Bueno and their alleged cryptocurrency trading activity. To vindicate the constitutional interests at stake, this Court should suppress all evidence obtained from Google or, alternatively, hold an evidentiary hearing pursuant to *Franks v. Delaware*, 438 U.S. 154 (1978), to develop a complete record as to Dias's state of mind when he submitted his misleading affidavits and the materiality of his many misrepresentations.

BACKGROUND

On January 5, 2024, IRS-CI Special Agent Dias swore an affidavit in support of a search warrant to Google for vast troves of stored electronic information—specifically, "all content and other information" associated with six email accounts that Dias believed to be associated with Defendants Anton Peraire-Bueno and James Peraire-Bueno. Declaration of Katherine Trefz ("Trefz Decl."), Ex. 8 (hereinafter, "Dias Aff."), at USAO_000001115.

Less than one month later, on January 30, 2024, Dias swore another affidavit in support of a supplemental search warrant to Google for yet more information—this time, "web & app activity, search, Chrome, and browsing history," which includes "[a]ll records related to Internet search and browsing history" and all "devices" or "apps . . . used," as well as "Google Services data," which includes "all files and contents" associated with the target accounts, including Google Chat, Google Drive, Google Messages, and YouTube. Trefz Decl., Ex. 9 ("Dias Supp. Aff."), at

USAO_00000198-99. In support of that further request, Dias relied on "the probable cause outlined in [his] January 5, 2024 . . . Affidavit." *Id.* ¶ 10. He provided no additional information to establish probable cause.

In reliance on the sworn affidavits that Dias submitted and the factual assertions that he made therein, Magistrate Judge James L. Cott issued the initial warrant to Google, and Magistrate Judge Robert W. Lehrburger issued the supplemental warrant. The substantial returns from Google formed the proverbial headwaters of the criminal investigation that ultimately resulted in the pending Indictment, charging the Peraire-Buenos with conspiracy to commit wire fraud, wire fraud, and conspiracy to commit money laundering. *See* ECF 2.

The constitutional problem, however, is that Dias deliberately included extensive false information in his affidavits or, at a minimum, acted in reckless disregard for the truth of the incriminating but inaccurate allegations that he leveled against the Peraire-Buenos. Absent those material misstatements, the scant information that remains in the affidavits would not have established probable cause, and the warrants to Google would not have issued. Accordingly, all evidence obtained from Google, as well as all fruit of that poisonous tree, should be suppressed.

ARGUMENT

I. LEGAL FRAMEWORK

In *Franks v. Delaware*, 438 U.S. 154 (1978), the Supreme Court held that, to overcome the presumption of validity that attaches to a search warrant issued by judge, a defendant must:

> make[] a substantial preliminary showing that a false statement knowingly and intentionally, or with reckless disregard for the truth, was included by the affiant in the warrant affidavit, and if the allegedly false statement is necessary to the finding of probable cause, the Fourth Amendment requires that a hearing be held at the defendant's request.

Id. at 155-56, 171; *see United States v. Perez*, 247 F. Supp. 2d 459, 472 (S.D.N.Y. 2003) ("[A] defendant may challenge the validity of a search warrant issued on the basis of an affidavit that contained false information.") (granting motion to suppress).

At a *Franks* hearing, a defendant seeking "[t]o suppress evidence obtained pursuant to an affidavit containing erroneous information" must satisfy two requirements. *United States v. Lauria*, 70 F.4th 106, 125 (2d Cir. 2023) (citation omitted). First, the defendant must show "the claimed inaccuracies or omissions are the result of the affiant's deliberate falsehood or reckless disregard for the truth." *Id.* (citation omitted); *see United States v. Fuccillo*, 808 F.2d 173, 178 (1st Cir. 1987) (holding police officers "were reckless in not including in the affidavit information which was known or easily accessible to them" and "simply did not take every step that reasonably could be expected of them" (citation omitted)). Second, the defendant must establish "the alleged falsehoods or omissions were necessary to the issuing judge's probable cause finding." *Lauria*, 70 F.4th at 125 (citation omitted).

If, at the hearing, the defendant establishes by a preponderance of the evidence that (1) the affiant deliberately misled the court or recklessly disregarded the truth, and (2) with the affidavit's false information set aside, its remaining contents are insufficient to establish probable cause, "the search warrant must be voided and the fruits of the search excluded to the same extent as if probable cause was lacking on the face of the affidavit." *Franks*, 438 U.S. at 156; *see United States v. Leon*, 468 U.S. 897, 923 (1984) (suppression is "an appropriate remedy if the magistrate or judge in issuing a warrant was misled by information in an affidavit that the affiant knew was false or would have known was false except for his reckless disregard for the truth").

II. DIAS INCLUDED MANY DELIBERATE FALSEHOODS IN HIS SWORN AFFIDAVITS OR, AT A MINIMUM, ACTED WITH RECKLESS DISREGARD FOR THE TRUTH.

In his affidavits in support of the applications for search warrants to Google, Dias asserted "there is probable cause to believe" that the Peraire-Buenos engaged in a scheme to defraud their alleged "victims," all traders who used automated computer programs (known as "bots") to exploit other Ethereum users through sandwich attacks.

Specifically, Dias accused the Peraire-Buenos of proposing transactions on the Ethereum Network that they had no intention of executing and deliberately altering transactions that their alleged victims had proposed. *See* Dias Aff. ¶¶ 12, 17, 19. He also claimed that, as part of their "Exploit," the Peraire-Buenos intentionally targeted "more obscure cryptocurrency tokens." *Id.* ¶ 17(b). But as Dias knew and his own affidavits established, all these allegations were false. In addition, Dias deliberately manipulated diagrams depicting the flow of information of the MEV-Boost protocol on the Ethereum Network, *id.* ¶ 14(c)(6), and he falsely asserted the Peraire-Buenos "tampered" with the blockchain itself, *id.* ¶ 13(d), which is not only demonstrably incorrect but technologically impossible.

At a minimum, Dias, who claims to have extensive expertise in cryptocurrency matters, *see id.* ¶¶ 1, 3, 13, and to have consulted publicly available information that flatly contradicts his statements, *see id.* ¶¶ 16, 17, recklessly disregarded the misleading inaccuracies that litter his affidavits.[1] These inaccuracies compounded to present an overall misleading picture of a very

[1] Throughout his affidavit, Dias refers to the Peraire-Buenos as "hackers." Dias Aff. ¶¶ 12, 17(b), 17(c), 18(c), 18(f), 19. That characterization is completely baseless and patently prejudicial. As Dias knows, even under the allegations in the Indictment, neither Defendant "hacked" anything. In their alleged "Exploit," they did not allegedly alter any computer code or network protocol for the Ethereum blockchain. Nor did they allegedly gain unauthorized access to any computer systems, for example by using fake credentials or passwords.

different and more nefarious hacking-based offense than the offense that was ultimately charged based on the same alleged underlying transactions.

A. Dias falsely asserted the Peraire-Buenos baited their alleged victims by proposing transactions that they had "no intention of executing."

In applying for the search warrants to Google, Dias misled the court when he falsely claimed the Peraire-Buenos "sent requests for trades that *they had no intention of executing* (*e.g.*, the Honeypot Transactions)." Dias Aff. ¶ 19(i) (emphasis added); *see also id.* ¶ 17(b), (d) (discussing so-called "Honeypot Transactions"). Dias had no direct evidence of the Peraire-Buenos' "intention[s]," nor did he cite any such evidence in his affidavits. Rather, he relied entirely on circumstantial evidence. But that purported evidence, including the transactions themselves, refutes Dias's baseless allegations.

As Dias knew, or should have known from the "publicly available blockchain information" he purported to review in connection with his affidavits, *id.* ¶ 16, the "Honeypot Transactions" were all executed as the Peraire-Buenos allegedly proposed them, and like other finalized transactions on the Ethereum Network, they have been permanently and publicly included in the Ethereum blockchain.

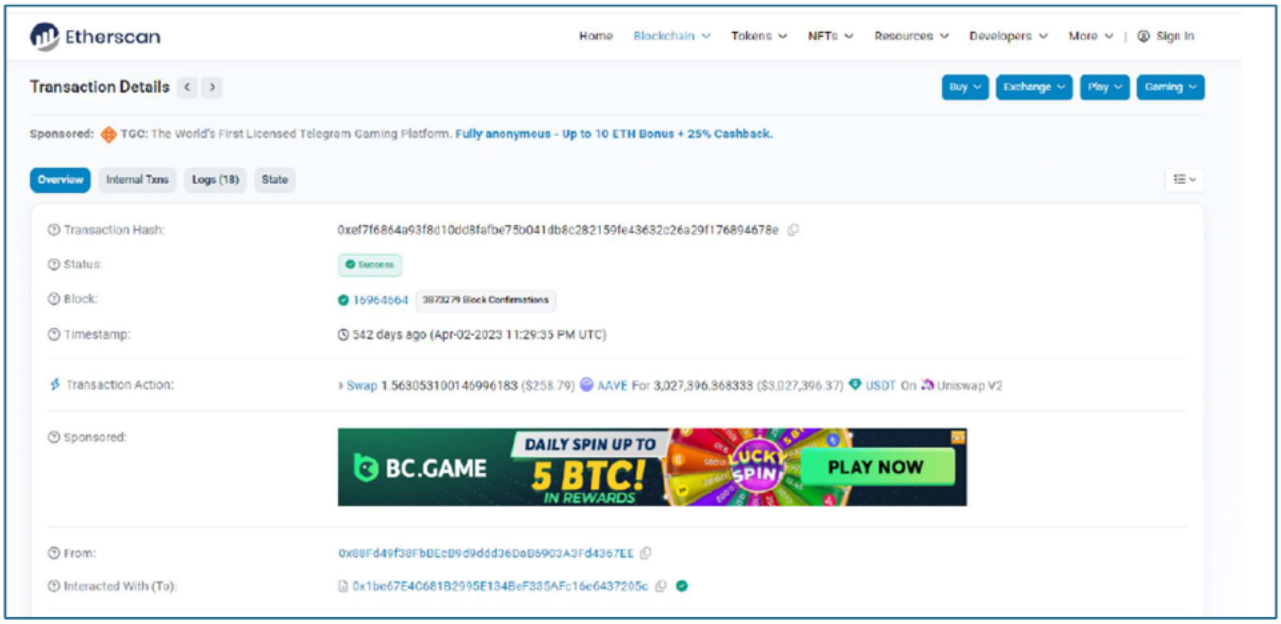
Consider the sole example in the warrant affidavit of a supposed sham transaction. *See id.* ¶ 17(f). According to Dias, in connection with the transactions by alleged "Victim-1," the Peraire-Buenos allegedly replaced their own "Honeypot Transaction" (swap of USDT for AAVE) with their own "Tampered Transaction" (swap in the other direction of AAVE for USDT). Disregarding the pejorative names, Dias is incorrect: the Honeypot and Tampered Transactions were all executed as the Peraire-Buenos allegedly proposed them. Dias knew that was the case, or recklessly disregarded those facts, because he reviewed the publicly available data regarding these transactions. Such data is available on Etherscan, an online blockchain explorer that can be used

like a search engine to review Ethereum data,[2] and was likely used by Dias to review and confirm transactions. *See id.* ¶ 17 ("Based on my review of publicly available information, including . . . blockchain scanners . . .").

Starting with the so-called Tampered Transaction, in his affidavit, Dias summarized the "swap" of AAVE, one of the most common tokens on the Ethereum Network, for USDT (or "Tether"), the largest stablecoin in the world which is pegged 1:1 to the U.S. dollar, as follows:

> **Tampered Transaction:**
>
> *Swap 1.563053100146996183 AAVE for 3,027,396.368333 USDT*

Dias Aff. ¶ 17(f). That basic information is included in the publicly available transaction details available on Etherscan.[3]



---

2 *What is Etherscan and how to use it?*, Coinbase, https://www.coinbase.com/learn/crypto-glossary/what-is-etherscan-and-how-to-use-it (last accessed Dec. 5, 2024).

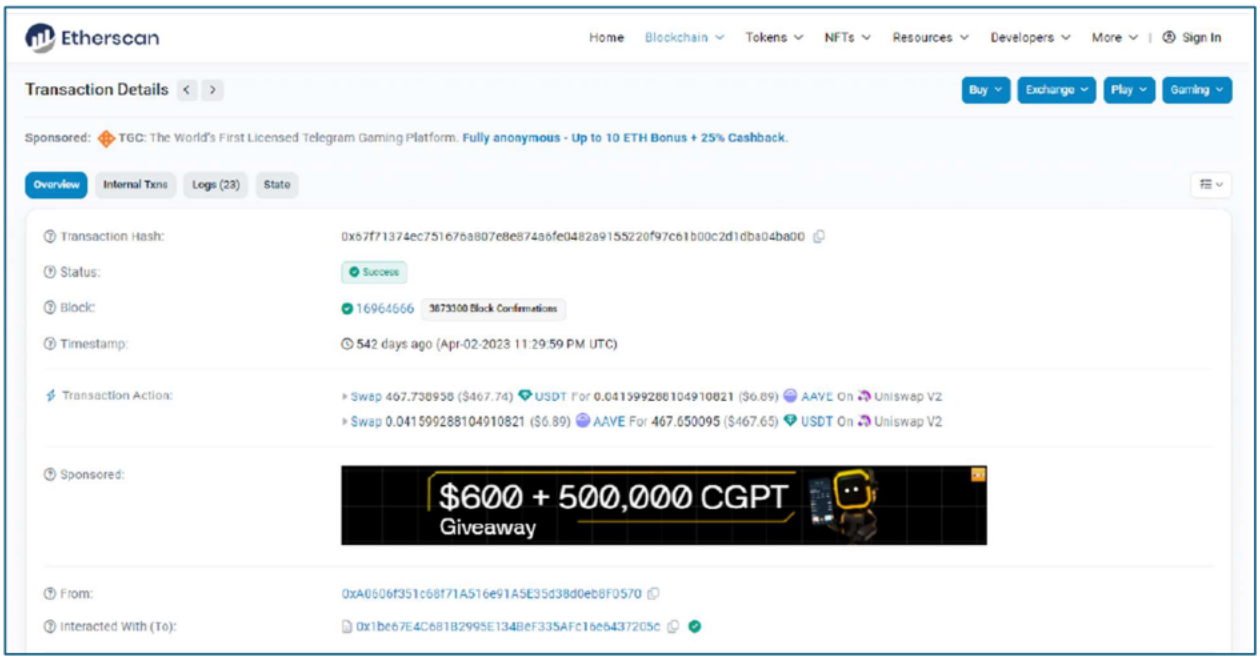
3 https://etherscan.io/tx/0xef7f6864a93f8d10dd8fafbe75b041db8c282159fe43632c26a29f176894678e (last accessed Dec. 6, 2024).

Etherscan confirms the "Tampered Transaction" was a "success" (*i.e.*, was executed) and included in Block 16964664 of the blockchain on April 2, 2023, at 11:29:35 PM UTC (or 6:29:35 PM EST).

Turning to the so-called "Honeypot Transaction," Dias summarized it as follows:

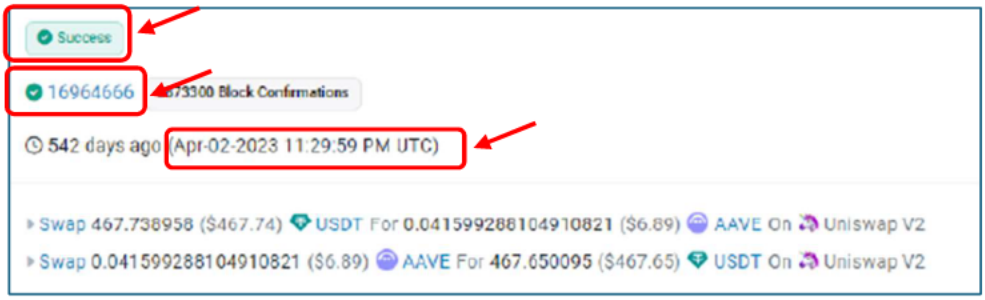
> **Honeypot Transaction:**
>
> *Swap 467.738958 USDT for 0.041599288104910821 AAVE*

Dias Aff. ¶ 17(f). Again, data about this transaction is publicly available on Etherscan.[4]



[4] https://etherscan.io/tx/0x67f71374ec751676a807e8e874a6fe0482a9155220f97c61b00c2d1dba04ba00 (last accessed Dec. 6, 2024)

As with the Tampered Transaction, the record of the Honeypot Transaction shows it, too, was a "success" and included only two blocks later in Block 16964666, which was proposed on April 2, 2023, at 11:29:59 PM, less than 30 seconds later and well within the standard inclusion time.



As this publicly available data makes clear, Dias's accusation that the Peraire-Buenos proposed transactions which they "never intended to execute" is false. Dias reviewed the records of these transactions, including the Ethereum blockchain itself, so he knew they were executed—or he should have known because the publicly available blockchain information he purported to review confirms it. These undisputed facts would have seriously undermined the incriminating story Dias presented in his affidavits.

B. Dias falsely accused the Peraire-Buenos of targeting "more obscure cryptocurrency tokens," even though the tokens at issue include some of the most valuable and common in the world.

In his affidavit, Dias claimed the Peraire-Buenos designed their so-called "Honeypot Transactions" to focus on "more obscure cryptocurrency tokens," mentioning among other tokens, Aave Token (AAVE) and Shiba Inu (SHIB). Dias Aff. ¶ 17(b). That inaccurate claim is, at best, remarkably uninformed.

Even a cursory review of publicly available information of the type Dias claimed to review confirms that AAVE, one of the tokens involved in the alleged transaction by "Victim 1," *id.* ¶ 17(f), is the token for the Ethereum Network's largest lending protocol, with a market capitalization in April 2023 of approximately $1 billion and a daily trading volume of

approximately $60 million.[5] AAVE, which launched more than 7 years ago (under its former name, ETHL) is now ranked 43rd on the list of over 10,300 active cryptocurrencies. SHIB was and is even bigger; in April 2023, it had a market capitalization of approximately $6.6 billion and a daily trading volume of approximately $367 million.[6] It is currently ranked 12th among all active cryptocurrencies.

By erroneously suggesting the Peraire-Buenos were operating in some small, dark corner of the cryptocurrency world, and trading in "obscure" tokens, Dias deliberately misled the court and painted a false picture of what he knew, or should have known, about the alleged "Exploit."

C. Dias falsely characterized the alleged victims as traders who specialized in "cryptocurrency arbitrage," but in fact, they were "sandwich attackers" who engaged in harmful market manipulation.

Dias misled the court when he falsely claimed, "the [alleged] Exploit targeted particular victims that specialize in high-frequency *cryptocurrency arbitrage trading*, which is designed to take advantage of *price differences* between identical or similar assets in *different markets*." Dias Aff. ¶ 11 (emphases added). As Dias knew, however, the transactions requested by the three alleged victims were not cryptocurrency arbitrage, but rather were intended "sandwich attacks." *See id.* ¶¶ 17(b) (referring to alleged victims' trades as "sandwich trades"), 17(h) (including schematics that referred to the alleged victims' trades as "sandwich attack[s]" or "sandwich attack bundle[s]"). As discussed in more detail in the Peraire-Buenos' Motion to Compel Production of *Brady* Material at 6-10 (filed today), the "sandwich attacks" in this case were not, as Dias falsely claimed, "designed to take advantage of price differences between identical or similar assets in different markets." Dias Aff. ¶ 11. To the contrary, unlike traditional arbitrage, the proposed trades—or

---

5 *See* https://coinmarketcap.com/currencies/aave/ (last accessed Dec. 4, 2024).

6 *See* https://coinmarketcap.com/currencies/shiba-inu/ (last accessed Dec. 4, 2024).

"attacks"—by the alleged victims were designed to manipulate prices within individual liquidity pools, *see id.* ¶ 13(h) (discussing liquidity pools), and "attack" other Ethereum users, who, as a result, swapped tokens at worse prices than they would have gotten if the "sandwich attack" had not occurred. *See* Motion to Compel Production of *Brady* Material at 6-8 (filed today). Sandwich trades like those the alleged victims sought to engage in are widely considered to be a form of market manipulation. *See id.* at 8-10.

The "frontrun" swaps that the alleged victims requested to start their sandwich attacks demonstrate that the supposed "victims" of the Peraire-Buenos' alleged "Exploit" set out to exploit unsophisticated retail users, not to make legitimate investments in any cryptocurrencies. As an example, consider the "MEV Bot Frontrun Trade" that Dias includes in his affidavit:

> **MEV Bot Frontrun Trade:**
>
> *Swap 3,027,389.579264 USDT for 0.089808338417418563 AAVE*

Dias Aff. ¶ 17(f). As noted above, USDT or "Tether" is a stablecoin pegged 1:1 to the U.S. dollar, and AAVE is a common token on the Ethereum Network. To execute this attack, the alleged victim in this case swapped a large amount of one cryptocurrency (USDT), which was worth more than $3,000,000, for a small amount of something else (AAVE), which was worth less than $7.[7] The absurd economics of that opening swap are an obvious tell that the alleged victim was playing a risky game, manipulating prices rather than investing in tokens.

[7] https://etherscan.io/tx/0x8ec2730e32319529ba084390e87c2f4384d69ce057bc1001daa6b8ac38be4ba9 (last accessed Dec. 6, 2024) (in the section for "ERC-20 Tokens Transferred," clicking on the grey button for dollar value of the second transfer, sending AAVE to the MEV Bot, shows the "estimated value on the day of transfer," which was $6.56).

D. Dias falsely claimed the Peraire-Buenos "altered transactions," but they are only accused of changing the *order* of requested transactions, not the terms.

Dias misled the court when he incorrectly alleged the Peraire-Buenos "deliberately altered certain transactions." Dias Aff. ¶ 19; *see id.* ¶ 16(f) (claiming Peraire-Buenos "alter[ed] certain transactions"). In fact, as Dias knows, the alleged "Exploit" did not, in fact, alter the terms of any proposed transactions. This is plainly true for two related reasons.

First, Dias's own affidavit identifies the alleged victims' trading strategy as a series of different transactions—*i.e.*, requests to swap specific tokens in specific amounts. *Id.* ¶ 11. As part of the alleged "Exploit," the Peraire-Buenos only stand accused of changing the *order* of potential transactions before including them in the block that they ultimately proposed to the Ethereum blockchain. The Peraire-Buenos are not accused, and never have been accused, of changing the terms of any requested transactions (*e.g.*, which token a particular user or wallet wanted to trade, how much of the token, at what price, or for what other token).

Second, the alleged harm to the victims does not stem from an allegation that the requested trades were altered; rather, it concerns their inability to exploit the "Honeypot Transaction"—which, as noted above, did ultimately execute in a different block—through their potential transactions. As explained above and in the Peraire-Buenos' Motion to Compel Production of *Brady* Material at 6-8 (filed today), the alleged victims in this case were all "sandwich attackers." To conduct their attacks, they sought to execute matched pairs of transactions (effectively, buy and sell trades) to "sandwich" another pending transaction by an unwitting retail user. By bundling their trades in this way, "[t]he blockchain attacker profits from the increase in the price from the previous transactions," which in the end, "results in a gain for the attacker and a loss for the user."

What is a Sandwich Attack, Uniswap.[8] Dias describes the recipe for a "sandwich attack" in similar terms, Dias Aff. ¶ 16(c)(i)-(iii), explaining that the "only valu[e]" of the bundle is the "sequential order," *id.* ¶ 16(c)(iii).

The charged scheme by the Peraire-Buenos supposedly frustrated the efforts by three sandwich attackers to prey on retail users of the Ethereum Network. But the fact that the sandwich attackers may have failed to attack their own victims does not mean that their trades were "altered" in any way by the Peraire-Buenos or prevented from proceeding. In the end, the initial front-run transactions and the later back-run transactions that the alleged victims submitted all executed as programmed by their smart contracts, and they have been included, along the Peraire-Buenos' alleged trades, in the Ethereum blockchain.

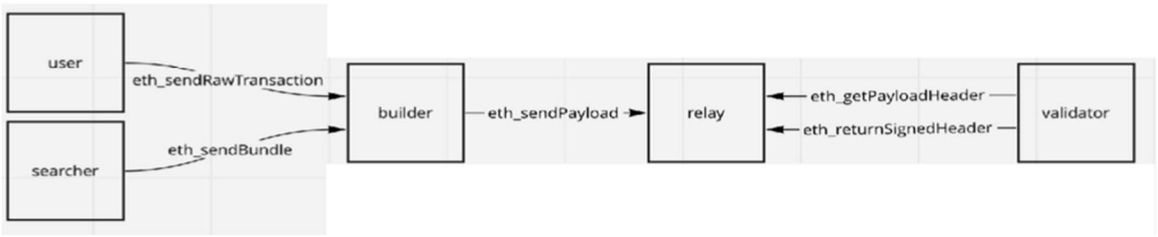
E. Dias manipulated a publicly available diagram of the MEV Boost application on the Ethereum Network to omit critical information that undermines the fraud allegations.

In his affidavit, Dias inserted a diagram of "executing a cryptocurrency transaction" on a decentralized exchange "using the MEV-Boost system" that erroneously suggests the relay does not provide any information to the validator. Dias Aff. ¶ 15(c)(6). Dias (or whoever gave the image to him) plainly obtained it from the internet, where Stephane Gosselin, the co-founder of Flashbots, posted the diagram on November 4, 2021, in a different form on his blog, HackMD.[9] The shaded background with visible gridlines confirms Dias cropped the original image to omit an important part of Gosselin's diagram—specifically, an "escrow" between the relay and the validator.

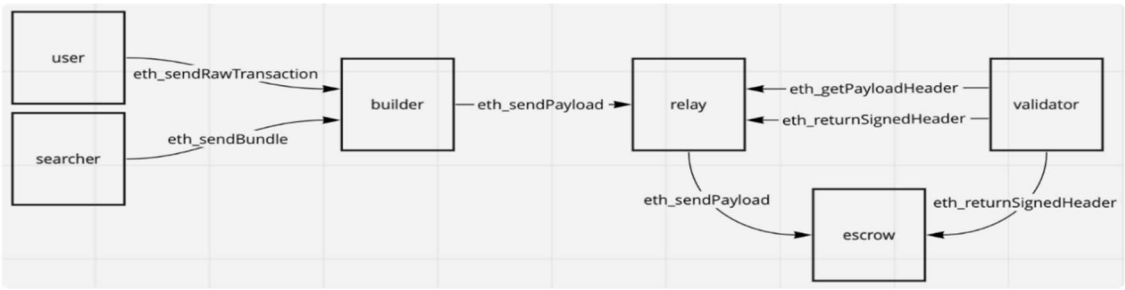
[8] *Available at* https://support.uniswap.org/hc/en-us/articles/19387081481741-What-is-a-sandwich-attack (last accessed Dec. 6. 2024).

[9] *Available at* https://hackmd.io/@flashbots/HJ3EbzVUY (last accessed Dec. 4, 2024).

Dias's altered image:



Gosselin's original image:



The difference is significant, and Dias's inclusion of the cropped version is misleading for a number of reasons. First, Gosselin's image depicted a proposed "architecture" for the MEV-Boost system that was not implemented, so the inclusion of the image at all is troubling. Second, Gosselin's image included an escrow, an additional party which would obtain all block information ("payload") from the relay and a digital signature ("signed header") from the validator. With that suggested design, the relay would only provide the block information to the escrow, not the validator, and the escrow would then propagate the validated block to the blockchain. In other words, in that proposal, the *relay* would *never* provide information directly to the validator.

But the MEV-Boost system did not adopt that design. The decision to use a process that does *not* include an escrow reflects the shared understanding of MEV-Boost users that the validator—not the non-existent escrow or any other party—will obtain block information from the relay. In other words, a validator that obtains such information has not "hacked" anything or, in

the parlance of the Computer Fraud and Abuse Act, gained "unauthorized access" to any computer system; it is expected for a validator to obtain information from the relay.

By cropping the escrow from his altered diagram and failing to explain the context of the original image, Dias hid from the court the undisputed fact that the validator appropriately receives information from the relay. His diagram falsely implied that in the regular process for proposing a potential block to the Ethereum blockchain, the validator provides a signature to the relay, but the relay does not provide any information to the validator, and therefore, it would be unexpected for the validator to receive any information from the relay. Indeed, his cropped image makes it appear that the relay does not release the block information ("payload") to any other party. That is incorrect, as Dias knew. *See* Dias Aff. ¶ 18(e) (acknowledging relay releases payload to validator). Far from evidence of any fraud or "hacking," the alleged transfer of block information from the relay to the Peraire-Buenos, as the validator, proceeded consistent with network protocols.

F. Dias falsely claimed the Peraire-Buenos "tampered" with the blockchain itself, but as Dias must know, that is not technologically possible, and all the transactions at issue remain on the permanent, public ledger.

Dias misled the Court when he falsely suggested the Peraire-Buenos somehow "tamper[ed]" with the "transparent and previously believed tamper-proof ledger system." Dias Aff. ¶ 13(d) (purporting to define "blocks" on a "blockchain"). It is true that a blockchain is transparent in that it consists of public information that anyone can access online. For example, anyone can see every block (and every transaction within every block) on the Ethereum blockchain by searching on a block explorer such as Etherscan.

It is also true that a blockchain is "tamper-proof," because once a new block is added to the chain, it cannot be altered or removed. In *Williams v. Binance*, 96 F.4th 129 (2d Cir. 2024), the Second Circuit recently discussed this central feature of a cryptocurrency blockchain.

> As with most crypto-assets, ownership of the Tokens is tracked on a blockchain, a decentralized ledger that records each transaction. . . . A critical difference [from banks] is that blockchains typically operate through a decentralized process: every computer running on a given blockchain independently tracks and clears transactions to validate the crypto-asset's ownership. Blockchains therefore allow for increased security, because *the decentralized nature of a blockchain means that any data recorded on the ledger cannot be altered.*

Id. at 134 (emphasis added); *see also United States v. Gratkowski*, 964 F.3d 307, 309 n.2 (5th Cir. 2020) ("Blockchain is a technological advancement that permits members in a shared network to 'record a history of transactions on an immutable ledger.'" (quoting Ashley N. Longman, Note, *The Future of Blockchain: As Technology Spreads, It May Warrant More Privacy Protection for Information Stored with Blockchain*, 23 N.C. Banking Inst. 111, 118-19 (2019))). As a technological matter, the Peraire-Buenos could not have changed any block on the blockchain.

Nothing about the alleged "Exploit" had any effect on the "tamper-proof ledger system," and Dias knew it. In his affidavit, Dias acknowledged that the alleged "Exploit" involved requested transactions *before they were added to the blockchain*—even while his affidavit also misleadingly suggests the opposite. For example, his affidavit describes "the execution of cryptocurrency transactions on DEXs" as follows: "When a user conducts a transaction on a blockchain network, such as a buy or sell trade, this transaction is not immediately confirmed. . . . A transaction is only considered final once it is included in a block that is published to the blockchain." Dias Aff. ¶ 14(a); *see also id.* ¶¶ 16(f), 17(g). Yet Dias also conveniently ignores this undisputed process when he tries to explain why the alleged "Exploit" was fraudulent: he states that the Peraire-Buenos "replaced approximately eight Honeypot Transactions in this manner on Block 16964664," *see id.* ¶ (e), misleadingly suggesting that block had been added to the blockchain earlier, when it had not.

Dias falsely claimed in his affidavits that the Peraire-Buenos "tampered" with the blockchain, and that baseless allegation was critical, because it supported the inflammatory claim

that their trading activity somehow undermined the "integrity" of the entire Ethereum Network. *See id.* ¶ 13(d).[10]

III. WITHOUT THE MANY FALSEHOODS THAT DIAS INCLUDED IN HIS AFFIDAVITS, PROBABLE CAUSE WAS LACKING TO ISSUE THE WARRANTS TO GOOGLE.

To determine the materiality of deliberate or reckless misstatements in a warrant affidavit, a reviewing court "correct[s]" the affidavit by excising the false information and determining whether the affidavit, as "corrected," establishes probable cause. *Lauria*, 70 F.4th at 125; *see United States v. Awadallah*, 349 F.3d 42, 70 n.22 (2d Cir. 2003) (noting that "a proper *Franks* inquiry" considers "whether the *remaining portions* of the affidavit give rise to probable cause" (emphasis in original) (citation omitted)); *see generally* W. LaFave, *Search and Seizure* § 4.4(c) at 24 (6th ed. 2021) ("[A]n affidavit with knowing falsehoods in it . . . should not be open to rehabilitation by a process of substituting for the affiant's lies other information that is really the truth from which he deliberately departed."). In this case, stripped of the many misrepresentations that Dias made, his affidavits do not establish probable cause to believe that the Peraire-Buenos engaged in wire fraud or conspired to do so (or any other crimes for that matter). Although probable cause is a relatively low bar, the affidavits fall far short of it.

The untainted remnants of Dias's affidavits establish only the following insufficient facts[11]:

---

[10] The Indictment against the Peraire-Buenos and the DOJ's press release about the pending charges made the same false claim about the "integrity" of the blockchain. *See* ECF 2, ¶ 1 (alleging that the Peraire-Buenos "exploited the very integrity of the Ethereum blockchain"); Dept. of Justice Press Release, Two Brothers Arrested for Attacking the Ethereum Blockchain and Stealing $25M in Cryptocurrency (May 15, 2024) (quoting U.S. Attorney Damian Williams, "As we allege, the defendants' scheme calls the very integrity of the blockchain into question."), *available at* https://www.justice.gov/opa/pr/two-brothers-arrested-attacking-ethereum-blockchain-and-stealing-25m-cryptocurrency.

[11] The Peraire-Buenos do not admit that these facts are true or that evidence concerning them would be relevant at trial. But for the limited, pre-trial purpose of the *Franks* analysis, the question

- The Peraire-Buenos were users of the Ethereum Network, on which they swapped cryptocurrencies.

- As part of the block proposal process on the Ethereum Network, the Peraire-Buenos also served as validators, which they were entitled to do pursuant to Ethereum's "proof-of-stake" protocols, because they staked the required amount of Ether, the native currency of the network.

- On the Ethereum Network, the Peraire-Buenos proposed "Honeypot Transactions," which were included by another validator in Block x666.

- On the same network, the Peraire-Buenos also proposed "Tampered Transactions," which they included as the proposers of Block x664 along with proposed transactions by the alleged victims.

- The alleged victims, all sophisticated "sandwich attackers," experienced trading losses.

- As validators, the Peraire-Buenos sent incomplete digital signatures to the relay on the Ethereum Network, and in response, the relay disclosed information about proposed transactions by the alleged victims in various bundles.

- Before proposing a new block to the Ethereum blockchain, the Peraire-Buenos switched the order of the potential transactions in the relay's delivered payload, but not the terms of those transactions.

- The transactions by the Peraire-Buenos did not involve altering any computer code or hacking any computer system.

- All of the transactions by the Peraire-Buenos are included in the Ethereum blockchain, which remains a tamper-proof, permanent, public ledger.

Those limited facts establish a markedly different record than the incriminating story that Dias told the court in his search warrant affidavits of a blockchain-tampering hack that stole cryptocurrency from on regular arbitrageurs.

With these remaining facts, no warrant should have issued. These limited facts do not establish probable cause that the Peraire-Buenos hacked anything. They do not establish that the

---

is whether the untainted facts that Dias included in his affidavits, if taken as true, were sufficient to establish probable cause for the challenged search warrants. They were not.

Peraire-Buenos undermined the integrity of the Ethereum blockchain—which is indisputably tamper-proof, despite Dias's false statements to the contrary. They do not (and could not) establish that the Peraire-Buenos altered the terms of any proposed transactions on the Ethereum Network. They do not (and could not) establish that the Peraire-Buenos proposed trades that they failed to execute (or never intended to execute in the first place)—one of the main arguments by Dias as to the means of a potential fraud. They do not establish that the Peraire-Buenos made any promises or statements to the alleged victims.

Instead, what remains of the Affiavit effectively accuses the Peraire-Buenos of outsmarting their alleged victims by frustrating those alleged victims' ability to complete their planned "sandwich attacks." But allegations of a failed attempt at market manipulation do not establish probable cause to believe the Peraire-Buenos committed wire fraud or any other crime.

CONCLUSION

For the foregoing reasons, Defendants Anton Peraire-Bueno and James Peraire-Bueno move to suppress all evidence obtained from the search warrants to Google, LLC, and all fruits of those poisonous trees, or alternatively, hold a *Franks* hearing.

Date: December 6, 2024

Respectfully submitted,

By: */s/ Katherine Trefz*

Katherine Trefz (*pro hac vice*)
Daniel Shanahan (*pro hac vice*)
Patrick J. Looby (*pro hac vice* pending)
Williams & Connolly LLP
680 Maine Avenue SW
Washington, DC 20024
Tel: (202) 434-5000
ktrefz@wc.com
dshanahan@wc.com
plooby@wc.com

Jonathan P. Bach
Shapiro Arato Bach
1140 Avenue of the Americas
17th Floor
New York, NY 10036
Tel: 212-257-4897
jbach@shapiroarato.com

Counsel for Defendant
James Peraire-Bueno

By: */s/ Daniel N. Marx*

Daniel N. Marx
William W. Fick (*pro hac vice*)
Fick & Marx LLP
24 Federal Street, 4th Floor
Boston, MA 02110
Tel: 857-321-8360
dmarx@fickmarx.com
wfick@fickmarx.com

Counsel for Defendant
Anton Peraire-Bueno

CERTIFICATE OF SERVICE

I hereby certify that on December 6, 2024, I electronically filed the foregoing document with the Clerk of Court using the CM/ECF system which will send notification of such filing to all counsel of record in this matter who are on the CM/ECF system.

/s/ Katherine Trefz
Katherine Trefz